WHAT IS CLAIMED IS:

1. In a computer system, a method comprising:

receiving a page comprising content including one or more elements; and

controlling page output and any actions corresponding to at least part of the content by:

1) interpreting at least one part of the page based on a first set of security settings; and

2) interpreting at least one other part of the page based on a second set of security settings associated with an element of the page, the second set of security settings being different from the first set.

2. The method of claim 1, wherein receiving the page includes accessing data received from a remote source.

3. The method of claim 1, wherein receiving the page includes accessing data received from a cache.

4. The method of claim 1, wherein a first action is requested in the content in the part of the page interpreted with the first set of security settings, wherein a second action that is similar to the first action is requested in the content in the part of the page interpreted with the second

set of security settings, and wherein controlling page output and any actions comprises, allowing the first action and disallowing the second action.

5. The method of claim 4 wherein the first action corresponds to a command to run a first set of script, and wherein the second action corresponds to a command to run a second set of script.

6. The method of claim 4 wherein the first action corresponds to a command to download a first set of data, and wherein the second action corresponds to a command to download a second set of data.

7. The method of claim 4 wherein allowing the first action comprises, prompting a user for a decision and receiving a response indicating that the action is allowed.

8. The method of claim 4 wherein disallowing the second action comprises, prompting a user for a decision and receiving a response indicating that the action is not allowed.

9. The method of claim 1, wherein a first action is requested in the content in the part of the page interpreted with the first set of security settings, wherein a second action that is similar to the first action is requested in the content in the part of the page interpreted with the second set of security settings, and wherein controlling page output and any actions comprises, disallowing the first action and allowing the second action.

10. The method of claim 1 wherein the first set of security settings are based on an identifier of the source of the page, and wherein interpreting at least one part of the page based on a first set of security settings comprises, retrieving the set of security settings based on the identifier, and associating the settings with the at least one part of the page.

11. The method of claim 10 further comprising, constructing a tree to represent the page, and wherein associating the settings with the at least one part of the page includes storing data corresponding to the security settings at a node in the tree.

12. The method of claim 1 wherein the wherein interpreting at least one other part of the page based on a second set of security settings comprises, recognizing security data associated with the element, and associating the second set of settings with the at least one other part of the page based on the security data.

13. The method of claim 12 further comprising, constructing a tree to represent the page, and wherein associating the settings with the at least one other part of the page includes storing data corresponding to the second set of security settings at a node in the tree that corresponds to the element.

14. The method of claim 13 wherein storing data corresponding to the second set of security settings comprises negotiating the second set of settings.

15. The method of claim 13 wherein negotiating the second set of settings comprises inheriting at least one setting in the second set based on security information associated with a parent node in the tree.

16. The method of claim 13 wherein negotiating the second set of settings comprises receiving at least one setting in the second set based on security information associated with a child node in the tree.

17. The method of claim 1, wherein controlling page output and any actions further comprises, accessing privacy settings.

18. A computer-readable medium having computer-executable-instructions for performing the method of claim 1.

19. In a computer system, a method comprising:

authoring a page containing at least one element; and

associating security data with an element contained in the page.

20. The method of claim 19, wherein associating security data with the element comprises, identifying a security zone.

21. The method of claim 19, wherein associating security data with the element comprises, identifying a file.

22. The method of claim 19, wherein associating security data with the element comprises, identifying a source of remote data.

23. The method of claim 19, wherein associating security data with the element comprises, providing a string of data corresponding to at least some of the security settings.

24. The method of claim 19, wherein associating security data with the element comprises, providing information indicating that the security settings should be determined relative to other security settings.

25. A computer-readable medium having computer-executable-instructions for performing the method of claim 19.

26. In a computer connected to a network, a system comprising:

browser software that interprets content received from the network, and

a security mechanism that associates a first set of security settings with a first part of the content, and associates a second set of security settings with a second

part of the content, the second set of security settings different from the first.

27. The system of claim 26 further comprising, a negotiator that controls the second set of security settings.

28. The system of claim 27 wherein the negotiator controls the second set of security settings relative to the first set of security settings.

29. The system of claim 28 wherein the negotiator controls the second set of security settings relative to the first set of security settings by having at least one setting in the second set be inherited from a corresponding setting in the first set.

30. The system of claim 26 wherein the first set of security settings is based on a network identifier of a source of the content.

31. The system of claim 26 wherein the first set of security settings corresponds to a security zone.

32. The system of claim 26 wherein the second part of the content corresponds to an element in the content.

33. The system of claim 32, further comprising a component that detects security data associated with the element.

34. The system of claim 33 wherein the security data associated with the element comprises, a reference to a security zone.

35. The system of claim 33 wherein the security data associated with the element comprises, a reference to a file.

36. The system of claim 33 wherein the security data associated with the element comprises, a reference to a source of remote data.

37. The system of claim 33 wherein the security data associated with the element comprises a string of data corresponding to at least some of the security settings.

38. The system of claim 33 wherein the security data associated with the element comprises information indicating

that the security settings should be determined relative to other security settings.

39. The system of claim 26 further comprising, a tree of nodes constructed from the content, the tree including a first node corresponding to the first part and a second node corresponding to the second part.

40. The system of claim 39 further comprising, a negotiator that controls the second set of security settings.

41. The system of claim 39 wherein the negotiator evaluates the second set of settings.

42. The system of claim 39 wherein the negotiator changes at least one setting in the second set of settings based on a rule.

43. The system of claim 39 further comprising, at least one other node in the tree that is associated with security settings based on inheriting information from a parent node.

44. The system of claim 43 wherein the parent node comprises the first node.

45. The system of claim 43 wherein the parent node comprises the second node.

46. The system of claim 39 further comprising, at least one other node in the tree that is associated with security settings based on security data of a child node.

47. The system of claim 26 wherein the second part of the content corresponds to a frame tag in the content.

48. The system of claim 26 wherein the content comprises an HTML page.

49. A computer-implemented method, comprising:

providing a page associated with a first security zone; and

providing an element in the page, the element being associated with a second security zone that is different from the first security zone.

50. The method of claim 49 wherein the element corresponds to a frame tag in the page.

51. The method of claim 49 wherein the first security zone comprises an internet security zone.

52. The method of claim 49 wherein the first security zone comprises an intranet security zone.

53. The method of claim 49 wherein the second security zone comprises a restricted security zone.

54. A computer-readable medium having computer-executable instructions for performing the method of claim 49.

55. A markup language document, comprising:

a first set of content associated with a first set of security settings; and

a second set of content associated with a second set of security settings, the second set of security settings being different from the first set of security settings.

56. The markup language document of claim 55 wherein the first set of content corresponds to a page, the second set of content is included in the page, and wherein the second set of security settings take precedence over the first set of

security settings with respect to determining security for the second set of content.

57. The markup language document of claim 55 wherein the first set of content corresponds to a page and the second set of content corresponds to a frame element included in the page.

58. The markup language document of claim 55 wherein the first set of security settings corresponds to a security zone.

59. The markup language document of claim 55 wherein the second set of security settings corresponds to a security zone.

60. The markup language document of claim 55, wherein the markup language document includes a reference to a file that corresponds to at least some of the second set of security settings.

61. The markup language document of claim 55, wherein the markup language document includes a reference to a source of remote data that corresponds to at least some of the second set of security settings.

62. The markup language document of claim 55, wherein the markup language document includes a string of data that corresponds to at least some of the second set of security settings.

63. The markup language document of claim 55, wherein the markup language document includes information indicating that at least some of the second set of security settings should be determined relative to other security settings.